Theoretical Computer Science 2 (1976) 397–400.

CIRCUIT SIZE IS NONLINEAR IN DEPTH

M.S. PATERSON
Department of Computer Science,
University of Warwick, Coventry, England

and

L.G. VALIANT
Centre for Computer Studies,
University of Leeds, Leeds, England

Communicated by A. Meyer
Received December 1975

Abstract. Two fundamental complexity measures for a Boolean function f are its circuit depth $d(f)$ and its circuit size $c(f)$. It is shown that $c \geqslant \frac{1}{4} d \cdot \log_2 d$ for all f.

1. Introduction

We consider acyclic Boolean circuits for $B_n = \{f \mid f\colon \{0,1\}^n \to \{0,1\}\}$ over the basis B_2. Two complexity measures can be defined for $f \in B_n$ as follows:

$c(f)$ = minimum number of gates of a circuit to compute f,

$d(f)$ = minimum depth of a circuit to compute f,

where the depth of a circuit is the maximum number of gates in a path of the circuit.

These measures satisfy the obvious relations

$$2^d > c \geqslant d,$$

and the example of n-argument conjunction demonstrates the optimality of the first inequality. In this paper we improve the second to $c \geqslant \frac{1}{4} d \cdot \log_2 d$ as $d \to \infty$.

McColl and Paterson [1] have shown that $d(f) \leqslant n+1$ for all $f \in B_n$. If f depends on all its n arguments then clearly $c(f) \geqslant n-1$ and therefore our result can be useful for only a small range of complexities. However, we hope that the proof method will be of interest.

2. Preliminaries

With any circuit $\mathscr{C}$, a directed acyclic graph can be associated in the usual way. Nodes of the graph correspond either to inputs or to logical gates. Let $e(\mathscr{C})$ be the number of arcs joining pairs of *gate* nodes in the graph of $\mathscr{C}$. We define

$$D(z) = \max\{d(f) \mid f \text{ is computed by a circuit } \mathscr{X} \text{ with } e(\mathscr{X}) \leq z\},$$

$$A(d) = \max\{z \mid D(z) \leq d\}.$$

Lemma. *For all $z > 0$, $D(z) \leq 1 + D(z-1)$.*

Proof. For any circuit $\mathscr{X}$ with $e(\mathscr{X}) = z > 0$, consider one of its gates that has only input variables as inputs, and replace this gate by a new input variable. The resulting new function is computed by a circuit $\mathscr{X}_1$ with $e(\mathscr{X}_1) \leq z-1$ and so has depth at most $D(z-1)$. It follows that $D(z) \leq 1 + D(z-1)$ since the original function requires a depth of at most one more. □

3. Main result

Theorem. *For all Boolean functions,*

$$c \geq \tfrac{1}{4} d \cdot \log_2 d - O(d).$$

Proof. Suppose $\mathscr{X}$ is a circuit of minimum size computing a function f at gate g_0, and suppose $e(\mathscr{X}) = z > 0$. We consider partitions of the gates of $\mathscr{X}$ into sets X and Y such that no gate of Y precedes a gate of X. If Y is non-empty then $g_0 \in Y$. Let $M \subseteq X$ be the set of gates of X adjacent to gates of Y and let $m = |M|$. We denote by $\mathscr{X}$ the circuit with X as the set of gates, and arcs and inputs as in $\mathscr{X}$. We denote by $\mathscr{Y}$ the circuit with Y as the set of gates, with the inputs of $\mathscr{X}$ together with new inputs corresponding to each node of M as its set of inputs and arcs as in $\mathscr{X}$. If $e(\mathscr{X}) = x$ and $e(\mathscr{Y}) = y$ then we have

$$x + y + m \leq z \tag{1}$$

since each node of M accounts for at least one arc from X to Y.

We wish to select a partition so that x and y are nearly equal. The transference of one gate from X to Y reduces x by at most two and m by at most one, therefore we may choose a partition such that

$$|2x + m - z| \leq 2. \tag{2}$$

If we define $v = \max\{x, y\}$, then from (1) and (2) we deduce that for some partition,

$$2v + m \leq z + 2. \tag{3}$$

Since $\mathscr{X}$ is a circuit for each of the functions computed at nodes of M, each of these may be computed in depth $D(x)$, by the definition of D. By composing these circuits with a minimal depth circuit equivalent to $\mathscr{Y}$ we can construct a circuit for f, which establishes

$$d(f) \leq D(x) + D(y) \leq 2D(v). \tag{4}$$

An alternative circuit for f is designed as follows. For each vector $c \in \{0,1\}^m$, replace each node of M (under some fixed ordering) in $\mathscr{Y}$ by the corresponding constant in c and simplify $\mathscr{Y}$ by absorbing these constants into the gates. Let $\mathscr{Y}_c$ be the resulting circuit and f_c the function it computes at g_0. Thus $d(f_c) \leq D(y)$. For each c, let δ_c be the function which is 1 if and only if the nodes of M in $\mathscr{X}$ have the values corresponding to c. These are just conjunctions of the (possibly negated) functions computed by $\mathscr{X}$ at the m nodes of M and so require depth at most $D(x) + \lceil \log m \rceil$. Using the identity

$$f = \bigvee_c \delta_c \wedge f_c,$$

we may produce a circuit for f establishing

$$d(f) \leq \max\{D(x) + \lceil \log m \rceil, D(y)\} + 1 + m$$

since the disjunction requires just m parallel steps.

Hence

$$\begin{aligned} d(f) &\leq D(v) + \lceil \log m \rceil + 1 + m \\ &\leq D(v) - 2v + z + 3 + \lceil \log m \rceil \quad \text{from (3).} \end{aligned} \tag{5}$$

In (4) and (5) we have two inequalities for $d(f)$ each defined in terms of the same fixed partition of $\mathscr{X}$.

Now we can suppose that f and $\mathscr{X}$ were chosen for some r so that $z = A(r) + 1$ and $d(f) > r$. Then (4) implies

$$D(v) > \lfloor \tfrac{1}{2} r \rfloor \quad \text{or, equivalently,} \quad v > A(\lfloor \tfrac{1}{2} r \rfloor). \tag{6}$$

By the lemma, the right-hand side of (5) is a decreasing function of v and it increases with m. Therefore it may be bounded above by taking $v = A(\lfloor \frac{1}{2} r \rfloor) + 1$ and $m = z + 2 - 2v$. Now by the lemma,

$$\begin{aligned} D(v) &\leq D(v-1) + 1 \\ &\leq \lfloor \tfrac{1}{2} r \rfloor + 1 \quad \text{since } D(A(d)) \leq d \text{ for all } d. \end{aligned}$$

Therefore from (5),

$$r < d(f) \leq \lfloor \tfrac{1}{2} r \rfloor + 1 - 2(A(\lfloor \tfrac{1}{2} r \rfloor) + 1) + z + 3 + \lceil \log z \rceil$$

or

$$z + \lceil \log z \rceil > 2A(\lfloor \tfrac{1}{2} r \rfloor) + \lceil \tfrac{1}{2} r \rceil - 2. \tag{7}$$

Since $z = A(r) + 1$, we have a recurrence inequality for the function $A(r)$ for arbitrary r. Let

$$H(r) = \tfrac{1}{2} r \cdot \log_2 r + 2 \log_2 r - kr,$$

then since

$$2H(\lfloor\tfrac{1}{2}r\rfloor)+\lceil\tfrac{1}{2}r\rceil-2>H(r)+1+\lceil\log(H(r)+1)\rceil$$

for all $k\geq 0$ and all sufficiently large r, we can prove by induction on r that for some k,

$$A(r)\geq H(r)=\tfrac{1}{2}r\cdot\log_2 r-O(r).$$

For any $\mathscr{X}$, $e(\mathscr{X})\leq 2c(\mathscr{X})$ and so we have proved

$$c\geq\tfrac{1}{4}d\cdot\log_2 d-O(d).\quad\square$$

Corollary 1. *For all functions, $d\leq O(c/\log c)$.*

Corollary 2. *For any sequence of functions $f_2, f_3, \ldots$ where $f_n\in B_n$ with linear circuit complexity, that is $c(f_n)=O(n)$, there is a constant A such that for all n, f_n can be represented by a formula of size $A^{n/\log n}$.*

Reference

[1] W. F. McColl and M. S. Paterson, Depth of all Boolean functions, *SIAM J. Comput.*, to appear.